



[WP-IC-005]

Arranging Fragility Within Systems

By Allan McDougall

Evolutionary Security Management, Inc.
BA, BMASc, PCIP, CAS
amcdougall@evolutionarysecurity.ca

and by Bob Radvanovsky

Infracritical, Inc.
CIFI, CISM, REM, CIPS
rsradvan@infracritical.com

ESM/IC CC License Version 1.1

Attribution. The licensors (Allan McDougall and Bob Radvanovsky) permits others to copy, distribute, display, and perform the work. In return, licensees (you) must give credit to either Allan McDougall and Bob Radvanovsky or Evolutionary Security Management and Infracritical, and the original author(s) of the material you use.

Non-Commercial. The licensor permits others to copy, distribute, display, and perform the work. In return, licensees may not use the work for commercial purposes – unless they get the licensor’s permission.

Share Alike. The licensor permits other to distribute original or derivative works, but only under a license identical to the one that governs the licensor’s work. Derivative works are Infracritical materials that have been edited, translated, combined with someone else’s

Exception. Certain elements (such as photos, graphs, text quotes) included within this document have been acquired from sources outside of Infracritical. Please contact the copyright owner to get permission for non-fair use purposes if you wish to copy, distribute, display, or perform an element that is not covered under the ESM/IC CC License.

The ESM/IC CC License follows licensing guidelines as outlined by Creative Commons standards:
<http://www.creativecommons.org>.

Questions should be addressed to:
info@infracritical.com

Table of Contents

Table of Contents	1
Authors’ Note about the Whitepaper	1
Objective	1
Introduction	2
Levels of Management.....	2
What is Fragility?	2
Definition of Reliability.....	3
What is Reliability Testing?	3
Definition of Natural Fragility.....	3
Definition of Cyclical Fragility	4
Definition of Potential Fragility	5
Definition of Capacity Fragility.....	7
Definition of Stability Fragility	7
Ice Storm Example.....	7
Conclusion.....	8

Authors’ Note about the Whitepaper

It is the intention of this whitepaper to convey to the general public the importance of properly defining and establishing terms and definitions used to determine methods of failure of any given system or infrastructure. Without establishing such a crucial elemental piece to the overall puzzle, the validity, more importantly, the security of our critical infrastructures depends upon an accurate method of describing how these systems fail. This paper hopes to address several of those issues.

Objective

The objective of this document is to provide a definition and criteria set of definitions outlining the overall perspective of what is ‘fragility’, how it is represented, and why it is important to the user communities. The document defines and outlines the following definitions (“fragility”) and reasons necessary for providing reliable systems and their measurement of this factor.

This document is by no means final or complete, but represents a conceptualization of a possible direction towards a securification methodology and practice model for an accurate and reliable infrastructure system, and is subject to review and discussion. Any and all questions, comments, critiques, et. al, are welcomed and should be directed to either **Allan McDougall** at Evolutionary Security Management (email: amcdougall@evolutionarysecurity.ca), or to **Bob Radvanovsky** at Infracritical (email: rsradvan@infracritical.com).

Introduction

Over the past ten years, several events have raised concerns regarding the stability of North America's critical infrastructures. In 1998 an ice storm left thousands without power during the winter and raised significant concerns about the electrical infrastructure in parts of Ontario and Quebec, Canada. This was further reinforced following the August 2003 blackout that left much of Eastern North America in the dark. The collapse of the *de la Concorde Bridge* in Montreal, Canada and the I-35W bridge failure/collapse left concerns regarding the state of many of the bridges in both Canada and the USA. The fire at the Nanticoke refinery left some communities without fuel and created transportation challenges as diesel shortages impacted the trucking industry. Finally, disruptions at major seaports have even lead to challenges in harvests in the central Canadian and USA heartlands. Following each of these events, questions and concerns are raised as to whether or not the remaining or restored infrastructure will perform as intended.

Levels of Management

Setting the stage, there are three levels that will be examined here. The tactical level can be described in terms of a local marine facility or port, a single entity operating at the local level. This level might also be described for those who use the mass transit system as a single bus stop—some are larger than others but generally it can be described as one single point in a network. The focus at the tactical level is on ensuring that the infrastructure at the facility is protected and that business continues. When moving from the local level to a regional level, one will be moving from the tactical to the operational level. The operational level focuses less on the protection of each and every single piece of infrastructure and moves towards the protection of capacity. For the mass transit user, a road may be closed. What is important is that the busses can bypass this closure and carry on down the route with minimal loss of capacity to move people from the suburbs to the downtown core. When moves from the regional to the national (or similar) level, one is moving from the operational to the strategic. The strategic level concerns itself as to whether or not the full system is meeting its goals and will often decide whether or not to adjust the demands or capacity offered by the system in order to protect that entire entity. For the mass transit user, this might involve the addition of routes to meet as-of-yet unaddressed demand or the closure of unprofitable routes. When discussing fragility, one must bear in mind the specific focus inherent in each level.

This discussion paper will center on the concept of fragility as the “propensity of the infrastructure to fail” in order to remain consistent with the scientific and/or technological definition of fragility that involves something becoming “brittle or easily broken.”¹ Fragility, in this respect, closely parallels the concept of risk in terms of risk being considered as either the “possibility of suffering harm or loss” or “the exposure to a chance of loss or damage” or operating in an “endangered state.”² Fragility, one might argue, approaches becoming synonymous with the risk of loss of availability due to failure.

What is Fragility?

This leads to a parallel (if in opposite directions) with the concepts behind Reliability Engineering. Reliability Engineering deals with the ability of “a system or a component to perform its required functions under stated conditions for a specified period of time.”³ Reliability Engineering also works within the realm of probability. In this case, however, we are looking at the probability that the infrastructure will fail. This can be linked through a basic mathematical equation where F represents fragility, R represents reliability and C represents 100 percent confidants:

$$F + R = C$$
$$F = C - R$$

This might be expressed literally as the fragility within the system is equal to the complete confidence in the system less the calculated reliability in the system. Fragility, like Reliability, would be represented in terms of a probability range of values. Where it is calculated that the Reliability is between 85% and 95%, the fragility would range between 5% and 15%.

¹ A general definition drawn from <http://www.answers.com/topic/fragility?cat=health>.

² These general definitions were drawn from <http://www.answers.com/risk?cat=biz-fin>.

³ This is a general definition drawn from http://en.wikipedia.org/wiki/Single_point_of_failure.

Definition of Reliability

The next consideration, however, is that Reliability is dependent upon time on two fronts. The first front represents the limit of the Reliability Test, often linked to the life cycle of the component. For example, given a Reliability Program (including monitoring, maintenance, etc), the component may be considered reliability 85% of the time through a life cycle of 20 years. The second linkage is represented within the Reliability Program that defines certain steps that must be taken in order to maintain the validity of the Reliability Test. For example, there may be a maintenance program that requires the changing of lubricants, etc.

On the mass transit front, this kind of activity is well-known and already practiced. The bus, for example, may have a life cycle of 20 years based upon a maintenance program after which it would have an anticipated failure rate that is unacceptable to the organization. This life cycle, however, is based upon maintenance routines and checks being conducted based upon so many hours of use, distance driven, or engine cycles. Should the organization decide to save costs by not performing two consecutive oil changes, the probability of failure increases as the number of engine cycles increases until the engine eventually fails.

What is Reliability Testing?

This is based upon specific values but the reality is that system will be in a constant state of flux depending upon the conditions. It is important to understand how the various variables in the Reliability Test interrelate with each other. For example, how does temperature affect the breaking point? How does the quality of the material affect the breaking point? The question becomes how does the temperature affect the breaking point given different qualities of material? Understanding these interrelationships becomes very important to understanding fragility.

This will invariably lead to two different approaches to testing. The first approach will involve the use of norms. Consider the mass transit example. Certain testing regimes will involve norms while others may be more detailed in nature. Consider mass produced parts and lubricants. It is likely that the testing will be based upon a sample of the overall population of parts—leading to norms being established. These norms will then be pushed forward in the Reliability Test and accepted as a relatively accepted. Other components will be tested individually in order to assure that they will function as anticipated. This is most notable in safety systems and similar kinds of technologies. In these cases, the unique testing becomes susceptible to narrower testing parameters due to the nature of the tester, the test equipment available and the volume of tests to be performed.

As a result, the first set check regarding confidence in the Reliability Testing process can be identified. The Reliability Test will likely involve one of two methodologies. The first involves testing a sample of a population and using the results across the full batch produced. This methodology makes the assumption that the full batch produced will not deviate significantly from certain standards. As a result, the Quality Assurance program of organizations using this methodology will provide a level of assurance as that program is intended to ensure that the end product meets the design standards as closely as possible. The second method involves the testing of each item, such as is often done with safety or environmental control systems. In these systems, the Quality Assurance program provides one level of assurance. The second consideration involves a Quality Assurance check associated with the competence of the tester, the quality (including calibration) of any testing equipment, the accuracy/detail of information recorded and the quality associated with the procedures to be applied.

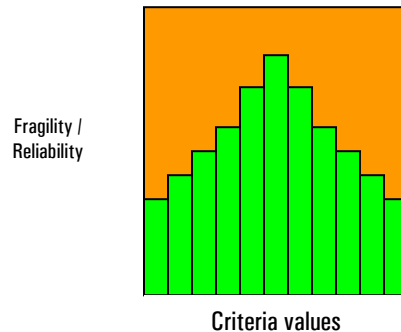
Definition of Natural Fragility

This leads to the first kind of fragility or what we will call "*natural fragility*". This is based upon the fact that the fragility is "expected and accepted."⁴ Within the structures of Reliability Engineering, testing is done based upon the probability of each component or input remaining reliable (over time and given conditions—this will come back later). By using the mathematical formula above and defining the fragility in terms of the conditions for the Reliability Test, we can set the parameters for the Fragility Test. Thus, if an engine is expected to be "90% reliable over a period of ten years as long as the Reliability program is followed and it is not subjected to conditions outside of the following" can be translated into the fragility of the engine being at 10% given the same constraints.

⁴ This is a general definition drawn from <http://www.thefreedictionary.com/natural>.

Definition of Cyclical Fragility

It is important to note that *natural fragility* must be transformed into "*cyclical fragility*". Cyclical fragility takes into account the changing environments that are relevant to the fragility calculation. Consider the oil being used as a lubricant on a bus within our mass transit system. The oil is reliable 90 percent of the time at 0 degrees (32 degrees for the USA). Now consider that the oil will also be used at minus 32 degrees (0 Fahrenheit) and plus 32 degrees (approximately 89.6 F). Given that the oil's characteristics and qualities change with temperature, can the fragility be assumed to be the same? To have confidence, the outer limits of the extremes would have to be evaluated. Ideally, each value would be calculated. This would result in an understanding of fragility in terms of a curve:



Where the green represents Reliability as tested given a set of conditions, the Fragility (represented) by orange changes based upon the results of that Reliability test.

The greater number of columns, the more refined the area under the curve and therefore the greater the accuracy

For infrastructure that remains exposed to cyclical events, it is important to understand the full range of *natural fragility* inherent in the system. This is done to mitigate the risk associated with larger deviations from norms, such as would be found during extreme hot and cold temperatures.

Cyclical fragility involves primary and secondary events. Primary events have a direct event upon the infrastructure, such as climate, rainy seasons, etc. The changes in these conditions have a direct influence upon the characteristics of the infrastructure. Where activities are taken in response to the cyclical changes, consideration must also be given as to how these would influence the infrastructure. For example, the winter season in Ottawa involves moderate snowfalls but decisions were taken to use salt on roads in order to reduce the impacts associated with those snowfalls (usually traffic accidents). The salts used, however, lead to salt water leaching through the bridge structures and causing an increased rate of rust on metal parts. This had not been considered during the design phase of the bridge, leading to the early replacement of one structure.⁵

To this point, we have examined the concept of *natural* and *cyclical fragility*. *Natural fragility* can be based upon the engineering design principles while *cyclical fragility* takes that natural fragility and inserts the periodic and predictable changes to build a more complete picture. The reason for using *natural fragility* as part of the design process is the same as we would use for Reliability Testing—the setting of standards or benchmarks to ensure a baseline level of quality. *Cyclical fragility* provides a better, or more complete, picture of the fragility in the system by including representations of the environment in which the system is working. This method uses the same methodologies as those used for *reliability testing* but using the different conditions.

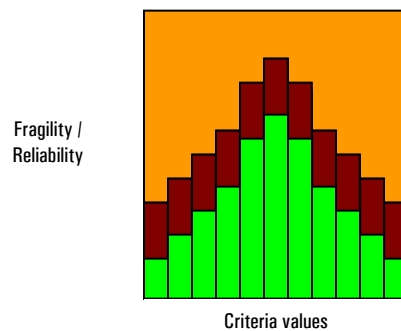
Events that impact the infrastructure can change the fragility associated with the infrastructure. One example can be found in the loading on aircraft wings.⁶ Basically, the cyclical loading on the wings can lead to micro-cracks in the structure that gradually reduces their effectiveness until they reach a point where the parts must be changed out or the aircraft retired from service. Now consider the rate of that loading. Given the normal load of the aircraft, one can expect a certain rate of deterioration. What if the aircraft were to experience wind-shear, turbulence, or other conditions that exceeded the "normal" load? A different impact is associated with those events.

⁵ One report on the story itself can be found at <http://www.canada.com/ottawacitizen/features/bridge/story.html?id=f20a75d0-bf6e-4076-be67-a924a5c62f66&k=98425>.
⁶ One discussion can be found at <http://www.greencarcongress.com/2007/09/new-material-fo.html>.

This leads to an understanding of the event in relation to the cyclical fragility. A three step approach is required here. First, is the impact of the event a constant across all conditions or does the impact change with changing conditions? This will speak to the overall influence of the event on the infrastructure. Having determined this factor, the next factor is how this influences the *natural fragility* of the system. This is an exercise in identifying clear cases where the impact would make the infrastructure unreliable. Should the infrastructure be considered reliable using the natural fragility, the next consideration is whether or not the impact has a different result using the *cyclical fragility*. This is done to identify conditions where a possibility of failure begins to enter into the realm of possibility. In our example regarding the aircraft wings, this would involve a situation where the aircraft was discovered to be slightly overloaded on a flight and the flight was subjected to the turbulence of a thunderstorm. The engineers responsible for identifying conditions would examine the *natural fragility* of the aircraft in relation to the event and determine that the aircraft was not operating under the stated conditions. They would then extrapolate the result using an understanding of the weight factor to determine whether or not there was a requirement to immediately pull the aircraft from service or whether or not an additional inspection of the aircraft was necessary (such as shortening the maintenance cycle). They would then also look at the *cyclical fragility* and apply the same methodology as used to the natural fragility into that system. In this case, it may well be determined that the extent of the turbulence under the additional weight conditions in those conditions causes enough concern to pull the aircraft for inspection. The results of the inspection would also be fed into the fragility model in an effort to ensure that the data being generated is valid.

Definition of Potential Fragility

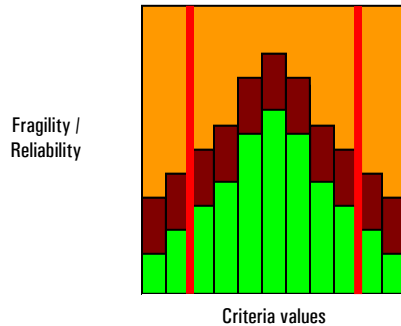
This kind of event leads to the next kind of fragility, referred to here as *potential fragility*. Like potential energy, *potential fragility* can be described in terms of the fragility stored within the system. This is an additional layer of fragility created on top of the *cyclical fragility* and is generally based upon either predictable factors such as aging or can be the result of the fragility created by an impact on the system. For example, in our example using aircraft, the additional strain on the wings may have caused additional micro-cracks in the structure that would cause it to be more susceptible to the next impact. This would be calculated by conducting the Reliability Test with the data using the characteristics of the system following the impact. In essence, this would appear in the following:



The dark areas represent the new fragility entered into the system due to an impact. This new fragility is the result of damage that did not reach the failure point but which does change how the system would likely respond to the next event. As a result, the overall fragility of the system increases.

It should be noted that the potential fragility does not have to be exactly the same under all conditions. A level of understanding of the impact across a range of conditions is necessary.

This *potential fragility* can have a significant impact by reducing the reliability in the system below tolerable levels. When linked to the extremes at either end of the Reliability results (often exhibited as the curve above), the conditions under which the infrastructure can be considered reliable is also reduced. Now consider that the Reliability of the infrastructure has approached the base of the curve (or zero on the chart above) when extrapolated. As this limit moves towards the reasonably predictable conditions, the infrastructure can be considered to be entering a period of fragility.



If the red lines represent the limit of reasonably predictable conditions (or a limit of risk tolerance with respect to conditions), as the fragility reaches zero to the outside of the lines the system would be *becoming increasingly fragile but within risk-managed levels*.

Where the *potential fragility* reaches zero within the boundary of the red lines, then the infrastructure can be declared to be *reasonably fragile*. While the fragility may not be apparent during periods of higher reliability, the increased potential for failure during extreme conditions would be identified.

Consider, for example, the situation with bridges. Built in the 1950's during a period of growth, the bridges were designed to handle approximately 100K cars per day during conditions between -50 degrees Celsius (-58 degrees Fahrenheit) and 50 degrees Celsius (122 degrees Fahrenheit) for a period of 25 years given a certain maintenance routine. When looking at the *natural fragility* in 2007, it is noted that the Reliability Test parameters had been breached some time ago. As a result, a bulletin was forwarded to the bridge authority indicating that a thorough inspection was necessary to determine if there were any immediate safety issues and a team dispatched. At the same time, using the extrapolated value, it was determined that the *natural fragility* might be within tolerable limits but, given the conditions and how they interact on the structure, *a concern existed with respect to cyclical fragility*, particularly where the structural integrity was reduced or increased loading was involved. Finally, upon review of the initial Reliability test assumptions, it was noted that *salt* was not factored into the equation. As a result, the added degradation of material (both Philly concrete and rebar having been studied) was factored into the equation. Using the increased rate of degradation and material decay, it was determined that the *potential fragility* of the infrastructure was well beyond tolerable levels and the bridge should be replaced at the earliest opportunity.

Up to this point, the concept of *fragility* has been restricted to the tactical level and expressed in terms of one aspect of the infrastructure. This is not a complete picture. One has to look at the capacity generated by that tactical infrastructure at the operational level. Consider one of two bridges crossing a river. If the total demand for crossing the river is approximately 200K vehicle-crossings per day and each bridge can handle 120K vehicle-crossings per day, then both bridges would be considered to be reasonably critical at the operational level. This is because the loss of any one bridge would lead to a result where the demands could not be met well into the long term—either the demand would have to be dropped or alternatives put in place (such as multiple temporary crossing points) to maintain the demand.

At the operational level, two kinds of *fragility* exist. The first involves the concept of *capacity fragility* and the second involves *stability fragility*. *Capacity fragility* examines the operational level in terms of redundancy, resiliency and robustness to meet the demand for capacity within the system. It examines whether or not the operational level is susceptible to single points of failure (or similar lacks of surplus capacity) that can make it susceptible to a single point of loss. *Stability fragility*, on the other hand, looks at the potential for loss of infrastructure within the operational level and the potential for fragmentation and dissolution of the system based upon the amount and nature of loss.

Definition of Capacity Fragility

At the operational level, *capacity fragility* is subject to both *natural fragility* and *cyclical fragility* issues. *Natural capacity fragility* at the operational level refers to the level of stored capacity within the system and how the system would be able to respond to the loss of capacity due to a failure of infrastructure. Consider the bridges above. In this example, neither bridge can meet the full demand of the system without going into an overload situation. Should one of the bridges fail, then the direct impact would be the loss of 80K vehicle-crossing per day. The method used to determine the potential severity of *natural capacity fragility* would involve the methods used for Regional Business Continuity Planning or Continuity of Operations Planning, as applicable. In this case, one might argue that the City Plan, and its reliance upon two bridges, has led to a reasonably fragile system as there is no surplus capacity within the system.

When looking at the issue from an operational perspective, the issue must also include any issues of *cyclical capacity fragility*. This represents losses of capacity due to predictable and periodic changes in the environment. For example, snow loading on the bridge may reduce the overall capacity of the bridge due to the added weight. Similarly, the capacity on the bridge may also be reduced as drivers are forced to reduce speed due to icing on the bridges. This *cyclical capacity fragility* at the operational level is handled the same way as *cyclical fragility* is handled at the tactical level as it stands in stead of the *natural fragility* when looking at "real world issues."

When looking at *cyclical capacity fragility* in the example above, the situation can be further exacerbated when the capacity of each bridge drops to 90K vehicle-crossings per day due to changes in climate involving increased snow seasons and ice seasons. In this circumstance, the system can be considered to be *capacity-fragile* as it cannot meet the periodic and predictable demands and the overall system has become a performance-limiter on the overall system.

Definition of Stability Fragility

The second level of fragility involves the *stability fragility* associated with the loss of network assets and infrastructure and how they would affect the overall stability of the system. This will depend significantly upon the topography of the network being looked at. Where the structure uses a number of spoke-and-hub configurations, the impact associated with the stability of the infrastructure must be balanced by the role that each node (such as an airport, transfer point, or station) or conduit (such as a route or transmission line) provides into the system. These issues have been the subject of much research recently and the mathematics has been evolving that allows for the rough prediction of how a regional network would first fragment and then potentially dissolve under continuous degradation.

The link between the tactical and operational levels occurs with the link between *tactical potential fragility* and *operational stability fragility*. The tactical level *potential fragility* indicates the propensity towards failure of a single point. This single point represents a node or a conduit in the operational-level network. The failure of one of these nodes or conduits at the operational level provides the trigger for the issue of *stability fragility* at the operational level. As a result, one can begin to represent the operational level for *stability fragility* in terms of the fragility across the tactical level that applies into the operational level.

Ice Storm Example

Consider an ice storm affecting the two bridges in the two-bridge fictional city. At the tactical level, the facility operator (bridge authority) understands that the ice storm would lead to the following impacts:

- * a relatively inconsequential addition of weight unless 100mm of freezing rain was received (at which point the loading of the bridge would be reached given traffic);
- * a requirement to reduce speed on the bridge to a point where only 80K vehicle-crossings would be possible; and
- * possible expansion of micro-cracks due to the ice being able to freeze and force expansion.

As a result of forecasting, it was understood that 90mm of freezing rain was expected over the next two days. The bridge authority therefore decided to salt all roads within 1km of the bridge approach and the bridge surfaces. As a result, the bridge engineer communicated that the design of the bridge was from before a period when salt was considered as an option. As a result, the rate of rusting of rebar and metal parts would be increased to a rate of approximately 20% faster than normal.

When looking at the *natural fragility* of the bridge, it was determined that the increased rate of rust out would lead to a condition where the *natural fragility* has breached the confidence threshold given a similar event the next year. It was therefore determined that a bridge upgrade would be needed the following year to reinforce the stringers and decking reinforcement before the next winter should it be salted.

At the operational level, two messages were received. The first involved the expected loss of capacity resulting from the storm, a factor that contributed to the *capacity fragility* at the operational level. The second was the change in *potential fragility* being below the threshold. This required a commitment of resources and effort to re-establish those comfort zones associated with the *potential fragility* but was going to result in a lane closure that was going to affect the overall capacity of the system.

At the strategic level, the changes in the operational level's *capacity* and *stability fragility* are weighed against the demand needed to be met if strategic requirements are to be made. In this case, the loss of capacity might be along a major route needed to meet some goal. The *potential fragility* of the infrastructure identified the specific kinds of work that need to be met in order to reduce the *stability fragility* at the operational level. It comes at a cost of *capacity fragility* that might pass acceptable levels due to the inability to meet demands. As a result, the strategic level puts in place alternatives that bypass the operational level in order to protect its own interests.

Conclusion

The concept of *fragility* cannot be logically separated across the three levels. They can be divided administratively or operationally, but logically the results from one will influence another. One method of expressing this fragility is in the form of matrices. At the tactical level, this would include the *cyclical and potential fragility*. At the operational level, it would include *capacity and stability fragility*. Once these four are looked at, information useful to the strategic level can be assembled.